REMARKS

I. Status of the Claims

Claims 26-50, of which claims 26 and 38 are independent, are pending and under examination.

II. Final Office Action

In the Final Office Action, the Examiner took the following actions:

(1) rejected claims 26, 27, 29, 38, 39, 41, and 50 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent App. Pub. No. 2003/0101353 ("*Tarquini*");

(2) rejected claims 28 and 40 under 35 U.S.C. § 103(a) as being unpatentable over *Tarquini* in view of European Patent App. Pub. No. EP 1330095 ("*Lahtinen*");

(3) rejected claims 30 and 42 under 35 U.S.C. § 103(a) as being unpatentable over *Tarquini* in view of U.S. Patent No. 7,301,899 ("*Goldstone*");

(4) rejected claims 31, 32, 43, and 44 under 35 U.S.C. § 103(a) as being unpatentable over *Tarquini* in view of U.S. Patent App. Pub. No. 2004/0015725 ("*Cole*");

(5) rejected claims 33, 34, 45, and 46 under 35 U.S.C. § 103(a) as being unpatentable over *Tarquini* in view of *Cole* and further in view of U.S. Patent No. 7,246,376 ("*Moharram*"); and

(6) rejected claims 35-37 and 47-49 under 35 U.S.C. § 103(a) as being unpatentable over *Tarquini* in view of *Moharram*.

III. Response to Rejections

Applicant respectfully traverses the aforementioned rejections and requests reconsideration based on the following remarks.

A. Claim rejections under 35 U.S.C. § 102(e)

The Final Office Action, on pages 2-7, rejected claims 26, 27, 29, 38, 39, 41, and 50 under 35 U.S.C. § 102(e) as being anticipated by *Tarquini*. Applicant respectfully traverses the

rejection because *Tarquini* does not disclose each and every element of the rejected claims. *See, e.g.,* M.P.E.P. § 2131.

Independent Claims 26 and 38

In particular, *Tarquini* does not disclose an intrusion detection system, for detecting unauthorised use of a network, comprising:

> a database storing attack signatures and, for each of the attack signatures, a set of at least one corresponding response signature; and
>
> a non-transitory computer readable medium encoded with a computer program product … including: ….
>
> instructions for a pattern matching engine for comparing the captured data with the attack signatures for generating an event when a match between the captured data and at least one attack signature is found, and
>
> instructions for a response analysis engine triggered by said event, for selecting, from the database, a selected set of at least one response signature corresponding to the at least one matched attack signature, and comparing, with the selected set of at least one response signature, response data being transmitted on said network as a response to said captured data and for correlating results of said comparisons with attack and response signatures for generating an alarm,

as recited in claim 26 (emphases added).

Tarquini at least does not disclose a database and a response analysis engine triggered by an event in the manner recited in claim 26. In its rejection of claim 26, on pages 3-4, the Final Office Action asserted that *Tarquini* discloses these features. Applicant respectfully disagrees with the Office's assertion.

Tarquini is generally directed to detecting an intrusion to a node of a network computer. *See Tarquini* at Abstract. The Final Office Action, on page 3, cited paragraph [0027] of *Tarquini* and associated databases 80A and 81A with the claimed database. Databases 80A and 81A of *Tarquini*, however, merely store "known attack signatures, or rules, against which network frames captured thereby may be compared." *Tarquini* at [0027] (emphasis added). Nowhere does *Tarquini* describe that databases 80A or 81A also store "a set of at least one … response

signature" as recited in claim 26 (emphasis added). Moreover, while paragraph [0048] of *Tarquini* mentions an outbound response signature maintained in a signature file, nowhere does *Tarquini* disclose that a database stores "for each of the attack signatures, a set of at least one corresponding response signatures" (emphasis added). That is, nowhere does *Tarquini* disclose that there is a correspondence between each of some attack signatures and some response signatures. Instead, as explained below, *Tarquini* deals with attack signatures and response signatures that are independent from each other, unlike those recited in claim 26.

Moreover, *Tarquini* does not disclose

> generating an event when a match between the captured data and at least one attack signature is found, and .... triggered by said event ... selecting ... a selected set of at least one response signature corresponding to the at least one matched attack signature, and comparing, with the selected set of at least one response signature, response data being transmitted on said network as a response to said captured data and for correlating results of said comparisons with attack and response signatures for generating an alarm,

as further recited in claim 26 (emphases added).

The Final Office Action, on pages 3-4, erroneously asserted that paragraph [0048] of *Tarquini* discloses these features. In paragraph [0048], *Tarquini* describes "detection of [an] inbound reconnaissance probe signature and a subsequent detection of an outbound response signature [which was] generated by the probed network stack in response to the probe packet." *Tarquini* at [0048]. *Tarquini*, however, does not disclose that first "an event [is generated] when a match between the captured data and at least one attack signature is found," and then "triggered by said event ... a selected set of at least one response signature corresponding to the at least one matched attack signature," is selected, and the steps of "comparing ... response data" and "generating an alarm" are performed, as recited in claim 26 (emphases added).

In *Tarquini*, contrary to the claim features, the detection of an outbound response signature is always performed and is not triggered by detection of a match between some inbound data and some attack signature. In fact, in *Tarquini* the reconnaissance probes are "indistinguishable from normal network traffic," and "appear to be legitimate TCP traffic, i.e. indistinguishable based on the inbound signature of the probe packet." *Tarquini* at [0041]. Thus, *Tarquini* "detect[s] reconnaissance probes ... by identifying the response to the packet probe by an outbound response signature." That is, *Tarquini* cannot distinguish a reconnaissance probe from legitimate traffic, and cannot generate an event in the manner recited in claim 26 merely by analyzing the inbound packets. Thus, *Tarquini* can only detect an attack after analyzing outbound response packets irrespective of any event.

Independent claim 38, although differing from claim 26 in scope, recites features similar to those discussed above in relation to claim 26. Therefore, for at least the above reasons, *Tarquini* does not disclose each and every element of claims 26 and 38, and thus does not anticipate these claims. Independent claims 26 and 38 should be allowable.

Claims 27, 29, 39, 41, and 50 each depend from, and thus incorporate features of, one of claims 26 and 38. Thus, for at least the reasons stated above in relation to claims 26 and 38, *Tarquini* also does not anticipate claims 27, 29, 39, 41, and 50. Claims 27, 29, 39, 41, and 50 should therefore be allowable by virtue of their dependence from base claim 26 or 38, and because they recite additional features not disclosed by *Tarquini*.

B. Claim rejections under 35 U.S.C. § 103(a)

The Final Office Action, on pages 7-12, rejected claims 28, 30-37, 40, and 42-49 under 35 U.S.C. § 103(a) over one or more of *Lahtinen*, *Tarquini*, *Goldstone*, *Cole*, and *Moharram*. Applicant respectfully traverses the rejection, noting that the scope and content of the cited art

have not been properly determined, and the differences between the claimed invention and the cited art have not been properly ascertained. Accordingly, the Office has not clearly articulated a reason why the cited art would have rendered the claims obvious to one of ordinary skill in the art. *See* M.P.E.P. § 2141.

Claims 28, 30-37, 40, and 42-49 each depend from, and thus incorporate the features of, claims 26 or 38. In its rejection of these claims, the Final Office Action relied on *Tarquini* for disclosures of the features of claims 26 and 38 and additionally cited *Lahtinen*, *Goldstone*, *Cole*, and *Moharram* for disclosure of features recited in claims 28, 30-37, 40, and 42-49. Regardless of whether these additional references disclose features asserted by the Office, which Applicant does not concede, the additional references do not cure the above-described deficiencies of *Tarquini* regarding the features of claims 26 and 38. That is, *Lahtinen*, *Goldstone*, *Cole*, and *Moharram*, whether considered separately or in any combination with each other and with *Tarquini*, do not teach or suggest an intrusion detection system, for detecting unauthorised use of a network, comprising:

> a database storing attack signatures and, for each of the attack signatures, a set of at least one corresponding response signature; and
>
> a non-transitory computer readable medium encoded with a computer program product ... including: ....
>
> instructions for a pattern matching engine for comparing the captured data with the attack signatures for generating an event when a match between the captured data and at least one attack signature is found, and
>
> instructions for a response analysis engine triggered by said event, for selecting, from the database, a selected set of at least one response signature corresponding to the at least one matched attack signature, and comparing, with the selected set of at least one response signature, response data being transmitted on said network as a response to said captured data and for correlating results of said comparisons with attack and response signatures for generating an alarm,

as recited in claim 26.

Moreover, despite the Final Office Action's assertions, *Lahtinen*, *Goldstone*, *Cole*, and *Moharram* also do not teach or suggest many of the features of the rejected claims.

Claims 30 and 42

Claims 30 and 42 recite generating the recited alarm "when said response data indicates that a new network connection has been established." In its rejection of claims 30 and 42 on pages 8-9, the Final Office Action agreed that *Tarquini* does not disclose these features, but asserted that *Goldstone* discloses them. Applicant respectfully disagrees with this assertion. The cited section of *Goldstone* merely describes that "[w]hen the router detects unusually high rates of new connections, it issues an alert message and then takes steps to control the flood." *Goldstone* at column 2, lines 58-60 (emphases added). Such disclosure of high rates of new connections and a flood does not, and the Final Office Action failed to specify how it does, correspond to the recited feature in which an alarm is generated as a result of detecting that one response data indicates establishing a new network connection.

Claims 31 and 43

Claims 31 and 43 recite that "said response signatures are arranged in two categories, response signatures identifying an illicit traffic, and response signatures identifying legitimate traffic." In its rejection of claims 31 and 43 on page 9, the Final Office Action agreed that *Tarquini* does not disclose these features, but asserted that *Cole* discloses them in its discussion of differently rated network vulnerabilities. Applicant respectfully disagrees with this assertion. The cited section of *Cole* merely describes rating network vulnerabilities on a low risk, medium risk, and high risk scale, which do not include the two recited categories. *See Cole* at [0361]. Moreover, network vulnerabilities merely relate to vulnerabilities of a configuration of network ports and an operating system. *See, e.g., Cole* at [0222]. Thus, contrary to the implied assertion

by the Final Office Action, network vulnerabilities do not, and the Final Office Action failed to explain how they do, correspond to the recited "response signatures."

Claims 35 and 47

Claims 35 and 47 recite "a time-out system triggered by said event for starting a probing task." In its rejection of claims 35 and 47 on pages 11 and 12, the Final Office Action agreed that *Tarquini* does not disclose these features, but asserted that *Moharram* discloses them. Applicant respectfully disagrees with the assertion. The cited sections of *Moharram* merely disclose a counter for the number of times a content identifier is requested. *See Moharram* at column 4, lines 12-15; column 5, lines 5-7; and Fig. 3 and its detailed description. *Moharram* does not, and the Final Office Action failed to specify where it does, teach or suggest a time-out system in the manner recited in claims 35 and 47.

Claims 36 and 48

Claim 48, which depends from claim 47, recites "generating the alarm in case only response signatures indicating legitimate traffic have been used; or ending said probing task in case only response signatures indicating illicit traffic or both response signatures indicating legitimate traffic and illicit traffic have been used." Also, claim 36, which depends from claim 35, recites features similar to those of claim 48. In its rejection of claims 36 and 48 on pages 11 and 12, the Final Office Action asserted that *Moharram* discloses these features. Applicant respectfully disagrees with this assertion. The cited section of *Moharram* merely discloses setting a threshold for a counter of a general content to be above the expected number of legitimate requests for the general content. *See Moharram* at claim 1. *Moharram* does not, and the Final Office Action failed to specify where it does, teach or suggest the above-recited

features based on whether or not only response signatures indicating legitimate traffic have been used.

Claims 37 and 49

Claim 37, which depends from claim 36, recites that "if such condition [as recited in claim 36] is not verified, said probing task attempts to perform a connection to a suspected attacked computer, for generating the alarm if such attempt is successful, or for ending the probing task if such attempt is unsuccessful." Claim 49, which depends from claim 48, recites similar features. In its rejection of claims 37 and 49 on page 12, the Final Office Action asserted that *Tarquini* discloses these features. Applicant respectfully disagrees. The cited section or any other section of *Tarquini* does not, and the Final Office Action failed to specify where it does, teach or suggest that an alarm is generated if a probing task attempt to perform a connection to a suspected attacked computer is successful, in the manner recited in claims 37 and 49.

Therefore, for at least the above reasons, claims 28, 30-37, 40, and 42-49 are patentable over *Tarquini*, *Lahtinen*, *Goldstone*, *Cole*, and *Moharram*.

IV. Finality of the Office Action

The Examiner, on page 12, indicated that the action is made final because Applicant's amendment necessitated the new ground(s) of rejection presented in the Final Office Action. Applicant respectfully disagrees because the new grounds of rejection were necessitated not by Applicant's amendments but by insufficiency of previous references cited by the Examiner. In particular, in the Office Action dated June 23, 2010, the Examiner rejected independent claims 26 and 38 under 35 U.S.C. § 103(a) as being anticipated by *Lahtinen* in view of *Dettinger*. However, as admitted by the Examiner during the Examiner Interview conducted on September 8, 2010 and reflected in the Examiner Interview Summary of September 10, 2010, *Dettinger*

does not teach the features on which the Examiner relied. This deficiency of *Dettinger* necessitated that the examiner withdraw the rejections, conduct a new search, and issue a new Action.

However, the Examiner requested Applicant file a response to the Office Action. While in the response of October 25, 2010 Applicant amended the claims, those claim amendments did not alter the features based on which Applicant had traversed the rejections of claims 26 and 38. Applicant thus contends that the new grounds of rejection were not necessitated by Applicant's amendments but by the inadequacy of the disclosures by *Lahtinen* and *Dettinger* and by the Examiner's attempt to cure the deficiencies of *Lahtinen* and *Dettinger*. Accordingly, Applicant submits that the Office Action cannot be made final. *See, e.g.,* M.P.E.P. § 706.07(a).

Applicant further notes that the newly cited reference by *Tarquini* was known to the Examiner before the Final Office Action dated January 5, 2011, as evidenced by the Examiner's reference to *Tarquini* in the Examiner Interview Summary of September 8, 2010. Nevertheless, *Tarquini* was cited in the Final Office Action for the first time. Because an Examiner is obligated to cite the best references at his or her command (*see, e.g.,* 37 C.F.R. § 1.104*; see also,* M.P.E.P. §§ 706, 706.02(I)), Applicant respectfully contends that to fulfill that obligation, the Examiner must provide Applicant with the opportunity to traverse *Tarquini* without filing a Request for Continued Examination.

V. Conclusion

Applicant respectfully requests the Examiner's reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 2, 2011

By: _____
Reza Sadr, Ph.D.
Reg. No. 63,292
(617) 452-1653